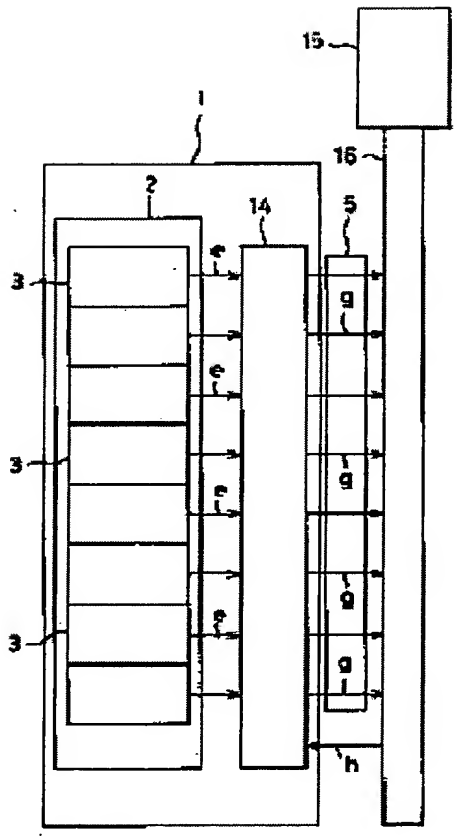
8-BIT RANDOM NUMBER GENERATOR

Patent number:	JP9097170
Publication date:	1997-04-08
Inventor:	ITO TORU
Applicant:	NIKO DENSHI KK
Classification:	
- international:	G06F7/58
- european:	
Application number:	JP19950255217 19951002
Priority number(s):	JP19950255217 19951002

Abstract of **JP9097170**

PROBLEM TO BE SOLVED: To directly obtain and output an 8-bit random number signal from a binary random number generator. SOLUTION: This generator consists of an 8-bit random number generation part 2 where eight random number generation circuits 3 which output random number signals (e) obtained by digitizing a noise signal (a) are provided in parallel and an 8-bit parallel transmission part 14 which takes individual random number signals (e) as the input and obtains a binarized signal (g) by sampling respective random number signals (e) at the same point of time in accordance with a control signal (h) from the outside and outputs this signal (g) as an 8-bit random number output (f), thus generating the 8-bit random number output (f) easy to handle at an 8-fold conversional speed of the speed before.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－97170

(43)公開日　平成９年(1997)４月８日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　7/58			Ｇ０６Ｆ　7/58	Ａ

審査請求　未請求　請求項の数２　ＯＬ　（全 5 頁）

(21)出願番号　特願平7－255217

(22)出願日　平成７年(1995)10月２日

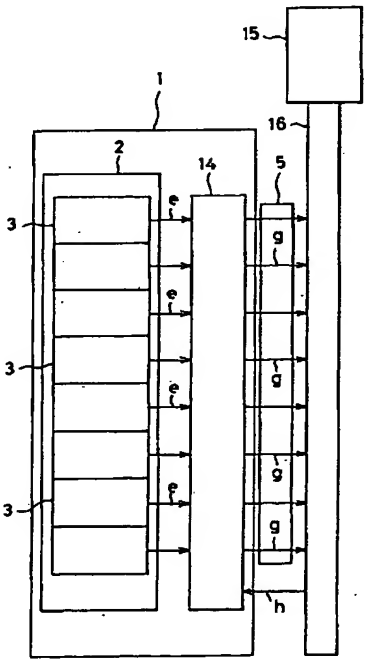
(71)出願人　391044292
ニコー電子株式会社
神奈川県横浜市港北区太尾町910番

(72)発明者　伊東　徹
神奈川県横浜市港北区太尾町910番地　ニコー電子株式会社内

(74)代理人　弁理士　渡辺　一豊

(54)【発明の名称】　８ビット乱数作成装置

(57)【要約】
【課題】　２進乱数作成装置から、直接に８ビットの乱数信号を得て、出力することにある。
【解決手段】　雑音信号ａをデジタル化した乱数信号ｅを出力する８つの乱数発生回路３を並列に設けた８ビット乱数発生部２と、各乱数信号ｅを個々に入力して、外部からの制御信号ｈに従って各乱数信号ｅを同一時点でサンプリングして得た２値化信号ｇを８ビット乱数出力ｆとして出力する８ビット並列送出部１４とから構成し、従来の８倍の速度で取り扱いの便利な８ビット乱数出力ｆを作成する。



1

【特許請求の範囲】

【請求項１】　直流成分を除去した確率的特性が既知であると共に、所定の帯域に制限されたガウス性電気雑音信号(a) をデジタル化した２進乱数信号(e)を出力する８つの乱数発生回路(3) を並列に設けた８ビット乱数発生部(2) と、該８ビット乱数発生部(2) の各乱数発生回路(3) からの乱数信号(e) を個々に入力し、演算装置(15)からの制御信号(h) に従って、前記各乱数信号(e) を単一のサンプリングパルスでサンプリングして得た２値化信号(g) を８ビット乱数出力(f) として演算装置バス(16)に出力する８ビット並列送出部(14)と、から成る８ビット乱数作成装置。

【請求項２】　各乱数発生回路(3) におけるガウス性電気雑音信号(a) の発生源を、ノイズツェナーダイオード(5) とした請求項１記載の８ビット乱数作成装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、システムのランダムデータによるシュミレーション、システムパラメタのランダムな選択、或いはデジタル情報のランダムな符号変換等に利用される８ビット乱数作成装置に関するものである。

【０００２】

【従来の技術】例えば、ノイズツエナーダイオードからの電子雪崩効果によって生成される電気雑音信号は、極めて低い周波数（１０Hz程度）から数１０MHz帯程度まで電力スペクトラムが平坦なガウス性白色雑音であることが知られており、これを利用したアナログ雑音発生器が通信回線の情報伝送品質の特性試験等に使用されている。

【０００３】このアナログ雑音発生器からの出力信号はアナログ波形であるので、デジタル的信号の取扱いが主流となっている現在、システムパラメタのランダムな選択、デジタル情報のランダムな符号変換等への応用には、更に何らかの変換が必要である。

【０００４】この要望を満たすべく、確率的特性の既知であり、かつ所定の帯域に制限された電気雑音信号から、１と０の２値系列から成るデジタル形式の乱数信号を得る技術が提案され、２進乱数作成装置として、暗号化用の乱数鍵やパスワード等の作成のために使用されている。

【０００５】

【発明が解決しようとする課題】しかしながら、従来の２進乱数作成装置により、コンピュータ等の演算装置で最も処理のし易い８ビットの乱数信号を得るには、２進乱数作成装置から出力された乱数信号を８回繰り返してサンプリングしなければならず、８ビットの乱数信号を得るのに面倒な手間と処理とが必要であると云う問題があった。

【０００６】また、従来の２進乱数作成装置が発生する

2

乱数信号の速度は、最高で１０MHzであるため、発生する乱数信号の波長に近い速度でサンプリングすると、同一波長内の値をサンプリングする場合が生じ、サンプリングした値がランダムではなくなってしまうことを考慮して、乱数信号発生速度よりも或る程度低い速度でサンプリングを行う必要があり、このため８ビットの乱数信号を作成するには、１ビットの場合の８倍以上の時間が必要となると云う問題があった。

【０００７】すなわち、図６に示すように、一つの乱数発生回路３で構成された２進乱数作成装置から出力された一つの乱数信号ｅから８ビット乱数出力を得るには、図７に示すように、出力された乱数信号ｅを第１のサンプリングパルスｂ１から第８のサンプリングパルスｂ８により１ビット毎の直列採取を行う必要があり、サンプリングパルスｂによる採取を開始してから、サンプリングパルスｂの時間間隔の少なくとも８倍の時間後の第８のサンプリングパルスｂ８による採取が完了した時点で、８ビット乱数出力（図７の場合、〔１００１１１０１〕、１６進数では９Ｄ）を得ることになり、各サンプリングパルスｂのサンプリングにより得た２値化信号を順に記憶する回路構成を必要とすることになっていた。

【０００８】そこで、本発明は、上記した従来技術における問題点を解消すべく創案されたもので、２進乱数作成装置から直接８ビットの乱数信号を得ることを技術的課題とし、もって演算装置における乱数信号の利用を容易なものとすると共に、速やかで円滑な乱数信号利用状況を得ることを目的とする。

【０００９】

【課題を解決するための手段】上記技術的課題を解決するため、本発明のうち、請求項１記載の発明は、直流成分を除去した確率的特性が既知であると共に、所定の帯域に制限されたガウス性電気雑音信号ａをデジタル化した２進乱数信号ｅを出力する８つの乱数発生回路を並列に設けた８ビット乱数発生部を有すること、この８ビット乱数発生部の各乱数発生回路からの乱数信号ｅを個々に入力し、演算装置からの制御信号ｈに従って、各乱数信号ｅを単一のサンプリングパルスでサンプリングして得た２値化信号ｇを８ビット乱数出力ｆとして演算装置バスに出力する８ビット並列送出部を有すること、を手段としている。

【００１０】請求項２記載の発明は、請求項１記載の発明の構成のうち、各乱数発生回路におけるガウス性電気雑音信号ａの発生源を、ノイズツェナーダイオードとしたことを手段としている。

【００１１】

【作用】請求項１記載の発明は、８つの乱数発生回路を並列に設けて８ビット乱数発生部を構成しており、各乱数発生回路から同期して出力された乱数信号ｅを、そのまま８ビット並列送出部に入力する。

【００１２】８ビット並列送出部は、一種のゲート回路

であって、外部の演算装置からの制御信号ｈの入力に従って、８ビット乱数発生部から入力された個々の乱数信号ｅを一つのサンプリングパルスでサンプリングして得た、すなわち１ビットの時間で得た、２値化信号ｇの組合せとして構成される８ビット乱数出力ｆを演算装置バスに出力する。

【００１３】このように、本発明による８ビット乱数作成装置は、１ビットの時間で、演算装置で処理し易い８ビットの信号である８ビット乱数出力ｆを演算装置側に出力するので、演算装置側における２値化乱数信号の取り扱いがきわめて容易となると共に、１ビットの時間単位で８ビット乱数出力ｆを得ることができるので、演算装置側における２値化乱数信号の取り扱い速度を大幅に高めることになる。

【００１４】

【実施例】以下、本発明の一実施例を、図１ないし図５を参照しながら説明する。図１は、本発明の８ビット乱数作成装置１の電気的構成の一実施例を示すブロック図で、８ビット乱数発生部２は、８つの乱数発生回路３を並列に設けると共に、各乱数発生回路３からの出力である乱数信号ｅは、そのまま８ビット乱数発生部２の出力として出力される。

【００１５】図２は、乱数発生回路３の電気的構成の一実施例を示すブロック図で、雑音信号発生部４と、Ａ／Ｄ変換器１０と、信号成形器１２とから構成され、一つのサンプリングパルス発生部１１が、各乱数発生回路３に接続されている。

【００１６】雑音信号発生部４は、電気雑音発生源としてノイズツェナーダイオード５を使用して図３に示す構成となっていて、図３において、６はノイズツェナーダイオード５に電子雪崩を起こすに適当な電流を流すための制限抵抗であり、７は直流分除去用のコンデンサであり、増幅器８の出力端子からノイズツェナーダイオード５から得た雑音信号ａが出力される。

【００１７】ノイズツェナーダイオード５から得られた雑音信号ａは、きわめて低い周波数（１０Hz程度）から数１０MHz程度までの電力スペクトラムが平坦なガウス性白色雑音であることが知られており、制限抵抗６の抵抗値および印加電圧値を選ぶことにより、通常、数１０μＡオーダーの電流をノイズツェナーダイオード５の供給電流としている。

【００１８】雑音信号発生部４からの雑音信号ａは、ローパスフィルタ９により所定の帯域に制限された後、Ａ／Ｄ変換器１０に入力される。

【００１９】Ａ／Ｄ変換器１０は、入力された雑音信号ａをサンプリングパルス発生部１１から入力されるサンプリングパルスｂでサンプリングし、このサンプリング値をＡ／Ｄ変換する。

【００２０】Ａ／Ｄ変換器１０による雑音信号ａのサンプリング値のＡ／Ｄ変換は、Ａ／Ｄ変換クロックパルスによって行われるが、このＡ／Ｄ変換クロックパルスの一つである最小桁クロックパルスｄにより、最小桁ビットに生起するデジタル信号である最小桁信号ｃだけを取り出し、この最小桁信号ｃを信号成形部１２を形成するフリップフロップ回路のＳ入力に入力する。

【００２１】信号成形回路１２を形成するフリップフロップ回路のもう一方の入力であるＲ入力には、Ａ／Ｄ変換器１０からの最小桁クロックパルスｄと最小桁信号ｃの反転信号とを入力するアンド回路１３の出力が入力されるので、信号成形回路１２であるフリップフロップ回路は、その出力状態と反対の最小桁信号ｃが入力される度に、その出力状態を反転させ、これにより２値化系列雑音信号である乱数信号ｅが生成されて出力される。

【００２２】各乱数発生回路３から出力される乱数信号ｅは、そのまま８ビット乱数発生部２の出力として８ビット並列送出部１４に出力されるので、８ビット乱数発生部２の出力信号は８ビット乱数系列となる。

【００２３】８ビット並列送出部１４は、８ビット乱数発生部２からの出力をそのまま受け入れて、外部からの指令である演算装置１５からの制御信号ｈにより、入力された８つの乱数信号ｅを単一時点でサンプリングして、各乱数信号ｅから２値化信号ｇを生成し、この２値化信号ｇをそのまま出力することにより、８ビット乱数出力ｆとして出力する。

【００２４】すなわち、図４に示すように、８ビット乱数発生部２の８つの乱数発生回路３から出力された乱数信号ｅは、図５に示すように、それぞれ同時に８ビット並列送出部１４に入力される。

【００２５】８ビット並列送出部１４に入力された各乱数信号ｅは、サンプリングパルスとして機能する演算装置１５からの制御信号ｈに従ってサンプリングされて、個々に２値化信号ｇに生成されると共に、そのまま８ビット乱数出力ｆとして出力されるが、例えば図５の場合は、第１の制御信号ｈ１により、第１の乱数信号ｅ１から０の２値化信号ｇが、第２の乱数信号ｅ２から１の２値化信号ｇが、第３の乱数信号ｅ３から１の２値化信号ｇが、第４の乱数信号ｅ４から１の２値化信号ｇが、第５の乱数信号ｅ５から０の２値化信号ｇが、第６の乱数信号ｅ６から０の２値化信号ｇが、第７の乱数信号ｅ７から１の２値化信号ｇが、そして第８の乱数信号ｅ８から１の２値化信号ｇがそれぞれ得られ、出力される８ビット乱数出力ｆは〔０１１１００１１〕となる。

【００２６】この８ビット乱数出力ｆは、サンプリングパルスとして作用する制御信号ｈの入力の度に出力されるので、この制御信号ｈとして従来からのサンプリングパルスを使用することにより、従来の８倍の速度で８ビット乱数出力ｆを得ることができることになる。

【００２７】８ビット並列送出部１４から出力された８ビット乱数出力ｆ、すなわち８ビット乱数作成装置１から出力された８ビット乱数出力ｆは、演算装置１５の演

5　　6

算装置バス１６に入力に入力され、そのまま処理される。

【００２８】

【発明の効果】本発明は、上記した構成となっているので、以下に示す効果を奏する。８つの乱数信号を一つの信号により単一時点でサンプリングして、各乱数信号を同時に２値化信号に生成し、この８つの２値化信号の組合せを８ビット乱数出力とするので、簡単にかつ正確に８ビット乱数出力を得ることができる。

【００２９】生成される８ビット乱数出力は、一つの信号による単一時点でのサンプリングにより得ることができるので、従来の８倍の速度で一つの８ビット乱数出力を得ることができる。

【００３０】８ビット乱数出力を直接出力するので、この乱数出力を入力するコンピュータ等の演算装置における８ビット乱数出力の取り扱い処理が容易で簡単なものとなり、きわめて扱い易いものとなる。

【図面の簡単な説明】

【図１】本発明装置の一実施例の電気回路構成を示す、ブロック図。

【図２】図１に示した実施例における、乱数発生回路の回路構成例を示すブロック図。

【図３】図２に示した乱数発生回路における、雑音信号発生部の回路構成例を示す電気回路図。

【図４】８ビット乱数発生部から並列出力される乱数信号の説明図。

【図５】８ビット並列送出部における８つの乱数信号から８つの２値化信号を生成する動作の説明図。

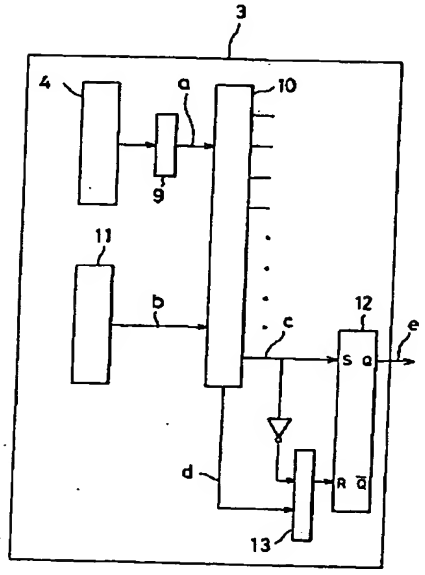
【図６】従来の乱数作成装置から出力される乱数信号の＊説明図。

【図７】図６で得た乱数信号から８ビット乱数出力を得る操作の説明図。

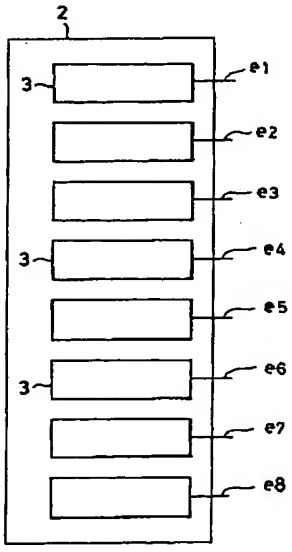
【符号の説明】

１　；　８ビット乱数作成装置
２　；　８ビット乱数発生部
３　；　乱数発生回路
４　；　雑音信号発生部
５　；　ノイズツェナーダイオード
６　；　制限抵抗
７　；　直流分カット用コンデンサ
８　；　増幅器
９　；　ローパスフィルタ
１０；　Ａ／Ｄ変換器
１１；　サンプリングパルス発生部
１２；　信号成形部
１３；　アンド回路
１４；　８ビット並列送出部
１５；　演算装置
１６；　演算装置バス
ａ　；　雑音信号
ｂ　；　サンプリングパルス
ｃ　；　最小桁信号
ｄ　；　最小桁クロックパルス
ｅ　；　乱数信号
ｆ　；　８ビット乱数出力
ｇ　；　２値化信号
ｈ　；　制御信号

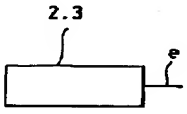
【図２】



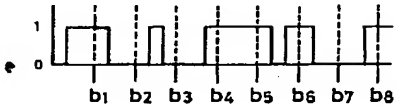
【図４】



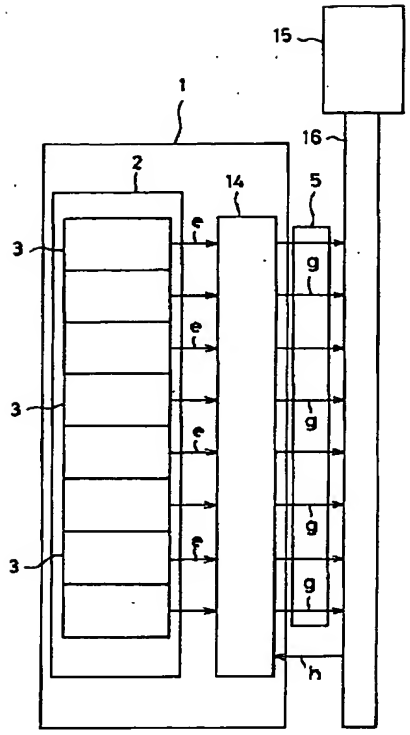
【図６】



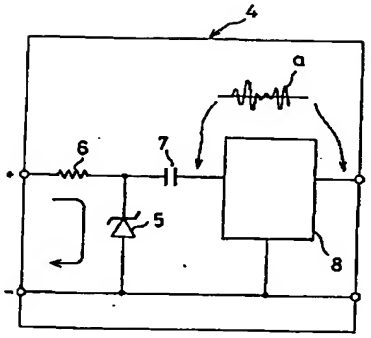
【図７】



【図1】



【図3】



1 ；8ビット乱数作成装置　2 ；8ビット乱数発生部　3 ；乱数発生回路
4 ；雑音信号発生部　5 ；ノイズツェナーダイオード　6 ；無抵抗
7 ；直流分カット用コンデンサ　8 ；増幅器　9 ；ローパスフィルタ
10；A／D変換器　11；サンプリングパルス発生部　12；信号成形部
13；アンド回路　14；8ビット並列送出部　15；演算装置
16；演算装置バス　a ；雑音信号　b ；サンプリングパルス
c ；最小桁信号　d ；最小桁クロックパルス　e ；乱数信号
f ；8ビット乱数出力　g ；2値化信号　h ；制御信号

【図5】